REMARKS

Claims 1-36 are pending in the present application. For the reasons presented below, applicant respectfully requests reconsideration of the rejection of these claims.

Claim Rejections - 35 USC §103

At section 5, claims 1-5, 7, 9-11, 17-21, 23, 25-26 and 31-37 are rejected under 35 USC §103(a) as unpatentable over US patent 6,970,565, Rindsberg, in view of US patent 7,149,901, Herbert, et al (hereinafter Herbert).

At section 6 regarding claims 1, 17 and 31-36, the Office reiterates the rejection set forth in the non-final Official Action of April 23, 2007. Specifically, it is asserted that Rindsberg teaches the actions in claim 1, except that it fails to specifically teach generating keys repeatedly. It is asserted that Herbert teaches generating, in a secure execution environment of an electronic device to which access is restricted, a new secret key repeatedly and using the new secret key for encryption of files to be stored.

The Office goes on to assert that at the time of the invention, it would be obvious to a person of ordinary skill in the art to utilize Herbert's key generation method with Rindsberg's secure downloading system, because it offers the advantage of increasing the strength of the encryption by using multiple keys with smaller data samples. Applicant respectfully disagrees for the reasons presented below.

More particularly, the disclosure of Rindsberg is considered by the Office to be the closest art. The Office as indicated above, alleges that Rindsberg fails to specifically teach generating keys repeatedly, but that it would obvious for a skilled person to incorporate Herbert's teaching of generating, in a secure environment, a new secret key repeatedly and using the new secret key for encryption of files to be stored.

Contrary to the position asserted by the Office at section 4 of the final Official Action, it is respectfully submitted that if a person of ordinary skill in the art at the time of the present invention would like to increase the security of the downloading and installation of patch programs to several devices, the suggested techniques available to a person of ordinary skill in the art based upon the method taught in Herbert in which new keys for encryption are generated at some points in time, could be used in combination

with Rindsberg although from the teaching in Rindsberg, it is clear that new key generation would be used for the shared key and not for the unique keys within the secure environment of the particular devices.

Specific reference is made to column 8, line 67 through column 9, line 8 of Rindsberg which states:

> "Since the shared key is typically known by a large number of devices, it is more likely to be compromised. Another reason that a second unique key is used is that the shared key may be changing at a relatively frequent rate. It is more efficient and practical to store the patch program encrypted using the permanent unique key rather than the transitory shared key. This is especially true considering that a patch program may be in a service for relatively long periods of time".

From this passage in Rindsberg, it is clear that since the shared key is typically known by a large number of devices, it is more likely to be compromised; that is, it would be more likely that a person of ordinary skill in the art would try to protect this relatively insecure key in an attempt to increase security. Furthermore, the disclosed permanent unique key is used because the shared key may be changing at a relatively frequent rate, which, one might argue, may introduce the concept that a new key generation according to Herbert might be useful.

However, such a modification to the unique permanent key is not obvious to one of ordinary skill in the art in view of the teaching of Rindsberg. The unique permanent key in Rindsberg is burned into the device during manufacture and represents a particular unique identification (ID) of the device (Rindsberg, column 7, lines 38-39). If this permanent unique key is changed, the device may no longer be identified as having that particular unique ID. Furthermore, as noted above with reference to column 8, lines 2-8 of Rindsberg, it is stated that the unique key is preferred to be permanent rather than transitory as is the shared key. Thus, there is no suggestion in the disclosure of Rindsberg toward having a repeatingly altered unique key.

This is in contradistinction to the argument presented by the Office at section 4 in response to applicant's arguments filed on July 23, 2007. At section 4, the Office asserts

that a person of ordinary skill in the art would have combined Rindsberg and Herbert to modify the unique key of Rindsberg repeatedly and to use the repeatedly modified unique key to re-encrypt the received patch program in spite of the fact that the unique key of Rindsberg is an identification number that is burned into the device during manufacturing. It should be emphasized that based upon the disclosure in Rindsberg, the unique key set forth therein has a functionality of identifying the device. To repeatedly change that unique key would in effect negate this functionality of the device disclosed in Rindsberg (see Abstract of Rindsberg). In fact, MPEP §2143.01 VI specifically addresses this situation. Section VI states:

> "VI The Proposed Modification Cannot Change the Principle of Operation of a Reference
>
> If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facia* obvious. *In re Ratti,* 270 F.2d 810, 123 USPQ 349 (CCPA 1959)."

Here, as in the cited *In re Ratti* decision, to modify the unique key in Rindsberg which represents an identification of the device with a periodically new key would effectively negate the identification property of the unique key disclosed in Rindsberg, which is set forth as being burned into the device during manufacturing. Furthermore, it should be noted that it would not be practical to repeatedly change such a unique key since, as pointed out above, each key (63) disclosed in Rindsberg corresponds to a particular ID (62) and is burned into the device during manufacturing (Rindsberg, Figure 2, column 7, lines 38-39). It is not practical, as would be apparent to one of ordinary skill in the art, to then re-burn such a key since the processing of burning into the device implies that it is stored in the device in a non-alterable fashion.

In short, a person of ordinary skill in the art, would not under any normal circumstances be motivated to change the burned in unique key repeatedly. Consequently, the particular combination asserted by the Office of using Herbert's repeating key generation with the unique ID key disclosed in Rindsberg would not in fact be possible nor obvious to a person of ordinary skill in the art at the time of the present

invention. Rather, as pointed out above, the repeating key capability of Herbert might provide a motivation in Rindsberg of repeatedly generating the shared key due to the fact that this shared key is discussed as being known by a large number of devices (Rindsberg, column 8, line 67 through column 9, line 2).

It is therefore respectfully submitted that claim 1 of the present application is not suggested by the combination of Rindsberg and Herbert.

For similar reasons, independent system claim 17 and independent system claim 36 are also not suggested by Rindsberg in combination with Herbert.

Dependent claims 2-5, 7, 9-11, 18-21, 23, 25, 26 and 31-35 are also not suggested by Rindsberg in view of Herbert due to their ultimate dependency from claim 1.

Furthermore, with regard to claims 2 and 18, the Office asserts at section 7 that Rindsberg as modified teaches a new secret key is generated when the device is booted (citing Herbert, column 8, lines 20-30, random number generator continually generates keying material). Claim 2, which depends from claim 1, states that a new secret key is generated when the device is booted.

Rindsberg discloses a method for securely downloading and installing a program patch in a processing device. The method disclosed in Rindsberg teaches:

- Patch contents are encrypted using a shared key known to all devices intended to receive the patch contents;
- Encrypted patch program is transmitted to the devices
- Patch program is then decrypted
- Patch program is checked for integrity, and if passed (integrity OK)
- Patch program is encrypted using a device unique key that is burned into the device during manufacture (Rindsberg, column 7, line 38-39)
- Encrypted patch program is transferred for storage in non-volatile memory

Upon reset or BOOT:

- The encrypted patch program is retrieved from the non-volatile memory
- The encrypted patch program is loaded into data RAM in the DSP
- Patch contents are decrypted using the device unique key
- The decrypted patch contents are loaded into patch RAM

- DSP begins operation using patch program installed in patch RAM

Thus, the received patch program is stored in RAM to enable rebooting of the device. If upon BOOT, the unique key was changed, the encrypted data could not be decrypted. Therefore, there are no indications that a person of ordinary skill in the art would take the teachings of Herbert, wherein new keys are generated repeatedly, and apply this concept to a solution according to Rindsberg.

Therefore, claim 2 is believed to be further distinguished over Rindsberg in view of Herbert. The same argument applies to dependent claim 18.

Furthermore, at section 12 regarding claim 9, the Office asserts that Rindsberg as modified teaches the step of generating a new secret key includes the step of generating a plurality of new secret keys, wherein each new secret key is used to encrypt a respective subset of data (citing Herbert, column 4, lines 20-30, random number generator continually generates keying material, column 4, lines 40-46).

Claim 9, which depends from claim 1, states that generating a new secret key comprises generating a plurality of new secret keys, wherein each new secret key is used to encrypt a respective subset of the data. However, it is seen at column 7, line 64 through column 8, line 3 of Rindsberg, that the contents of the patch program which are typically first encrypted using the shared key that is known to devices intended to receive the patch (step 90, Figure 3) may alternatively, for added security "be divided into groups whereby each group has a different shared key associated with it". The patch program is encrypted using the shared key for each group. Therefore, multiple transmissions are required in order to communicate the patch to all of the devices since each group has its own shared key.

It is clear from this portion of Rindsberg that the different shared keys discussed are with respect to encryption of data to be transmitted to the devices and therefore these keys are outside of the secure environment of the devices. This is contrary to the method claimed in dependent claim 9. Therefore, dependent claim 9 is believed to be further distinguished over Rindsberg in view of Herbert.

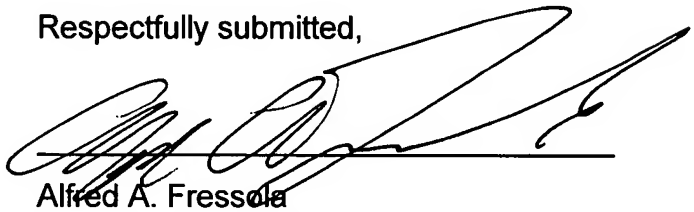
Remaining dependent claims 8, 24 (rejected at section 17), claims 14 and 27-28 (rejected at section 19), and claims 15, 16, 29 and 30 (rejected at section 23), are all

ultimately dependent from either method claim 1 or system claim 17 and are therefore believed to be allowable in view of the allowability of the independent claim from which they ultimately depend.

In view of the foregoing, it is respectfully submitted that the rejection of claims 1-36 as set forth in the final Official Action has been overcome and early allowance of the present application is earnestly solicited.

The undersigned respectfully submits that no fee is due for filing this Request for Reconsideration. The Commissioner is hereby authorized to charge to deposit account 23-0442 any fee deficiency required to submit this paper.

Respectfully submitted,



Dated: October 19, 2007

Alfred A. Fressola
Attorney for Applicant
Registration No. 27,550

WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON LLP
Bradford Green, Building Five
755 Main Street, P.O. Box 224
Monroe, CT 06468
Telephone: (203) 261-1234
Facsimile: (203) 261-5676
USPTO Customer No. 004955